DEFENSE INTELLIGENCE AGENCY

Department of Defense
Intelligence Management System

AIS SECURITY CERTIFICATION TEST REPORT

(DATE OF REPORT)

TEST PERIOD
24 January 1994

DoDIMS PMO
National Intelligence Production Center
DIA/PO-5C
Defense Intelligence Analysis Center
Washington, DC

Submitted by:

Approved by:

JOHN C. LEE, DIA/PO-5C Test Coordinator	JUDY C. CRISPELL, DIA/SY-ID Test Director
JEAN C. LAYTON, DIA/PO-5C Team Member	MICHAEL C. HOROWITZ Team Member

EXECUTIVE SUMMARY

A Computer Security Test supporting certification of the DoD Intelligence Management System (DoDIMS) was conducted by DIA/SY-1D on 24 January 1995 at the Defense Intelligence Analysis Center, Washington, DC. This testing demonstrated conformance to DIAM 50-4 and DCID 1/16 requirements for operation in the System High Security Mode of Operation at the TS/SCI level.

The test was based upon an approved test plan and was completed successfully with no major discrepancies noted. Minor discrepancies between the AIS design and national policies were noted and are included in the test report.

The purpose of the DoDIMS is to support the DoD and National intelligence communities in registering, validating, tracking and managing production requirements. It provides the mechanism for scheduling, deconflicting, assigning production and most importantly, provides the capability to track and manage overall production activities across operational and national planners and consumers. The DoDIMS program is structured under the definition of a DoDIIS Core product. DoDIMS will operate in the System High Mode at the Top Secret (TS), SCI Level.

The test team, with the concurrence of the Test Director, unanimously recommends final certification of the DoDIMS AIS, contingent upon satisfying the requirements specified in the Test Results section of this report for an AIS processing TS/SCI data in the System High Security Mode of Operation.

ACKNOWLEDGEMENT

The Test Director wishes to acknowledge the significant contributions which culminated in the highly successful and impressive certification test. The effort which was put into the preparation of the test plan, test conduct and test report preparation was obviously professional and much appreciated. In particular, the following personnel are acknowledged for their efforts during the test and test preparation period.

William H. Fleming, DoDIMS PMO, DIA/PO-5C
John C. Lee, DIA/PO-5C
Jean M. Layton, DIA/PO-5C
Tony Goe, J.G. Van Dyke & Associates, Inc.
Doug Hallford, J.G. Van Dyke & Associates, Inc.
Debbie Lambert, J.G. Van Dyke & Associates, Inc.
Harry Hiltz, J.G. Van Dyke & Associates, Inc.

1.0 (U) INTRODUCTION

The Department of Defense Intelligence Management System (DoDIMS) is a software application designed to support the DoD and National intelligence communities in registering, validating, tracking and managing production requirements. It provides the mechanism for scheduling, deconflicting, assigning production and most importantly, provides the capability to track and manage overall production activities across operational and national planners and consumers. The DoDIMS program is structured under the definition of a DoDIIS Core product. DoDIMS will operate in a system high mode at the Top Secret (TS), SCI Level.

1.1 (U) Purpose

DoDIMS is designed to provide members of the DoD and National intelligence community a common application to support the registration and tracking of intelligence requirements and production for General Military Intelligence, Current Intelligence and Crisis Intelligence, Scientific and Technical Intelligence, and Imagery Analysis.

1.2 (U) Systemic Functions

DoDIMS will function as a client server-application using Joint Deployable Intelligence Support System (JDISS) to host the DoDIMS application. Through a replication server process, each site DoDIMS will update other DoDIMS peer databases. Thus, a local site will have read/write capability of its data but read only capability of data concerning remote, peer sites. Eventually a master, read-only DoDIMS database will be established at the Defense Intelligence Analysis Center. The Joint World-wide Intelligence Communications System (JWICS) will provide the network support for DoDIMS client-server communications. Use of JDISS, a current operational and accredited system, will allow connectivity with other intelligence systems required to support users during peacetime, crises, and wartime. The DoDIMS user will, therefore, have an integrated and interoperable tactical intelligence capability that includes host access, electronic mail, message handling, image processing, motion video processing and graphics capability.

DoDIMS will receive input primarily from the user community. Users will be categorized as Requestors, Validators, and Production managers. User inputs will range in classification from unclassified to TS/SI/TK depending on the nature of the production request and/or query. User input will update the database by direct keyboard interface, mouse activation, and indirectly by the application environment, e.g., cut and paste. Updates of the database will be performed as a system administration function. Inputs for updating system tables will be by file transfer protocol (FTP), floppy diskette or 8mm tape.

The principal output will be visual via a display monitor. The classification level will be permanently displayed on each workstation defaulted to the highest classification level processed by the application. All hard copy output will be appropriately labeled at the top and bottom of each page.

Transactions, i.e., production requests, will be replicated by the COTS database software to applicable DoDIIS sites via JWICS/JDISS. Transaction replication will also be made to both peer

databases and the central DoDIMS server resident in the Defense Intelligence Analysis Center (DIAC). Should communication downtime occur, output to the central server will be stored and forwarded by each site's replication process upon re-establishment of the communication link.

DoDIMS will not accomplish sanitization or decompartmentation.

1.3 (U) Test Site Location

The DoDIMS AIS certification test was conducted in Room B5-935, DIAC, Washington, DC.

1.4 (U) Operational Environment

DoDIMS is a client-server application developed in accordance with DoD and DIA information system architectural standards. It consists of five client modules which reside on a Joint Deployable Intelligence Support System (JDISS) workstation and a database co-hosted on the same workstation. Eventually a master, read-only database will be established on a dedicated server at the DIAC.

DoDIMS will receive input primarily from the user community. Users will be categorized as Requestors, Validators, and Production managers. User inputs will range in classification from unclassified to TS/SI/TK depending on the nature of the production request and/or query. User input will update the database by direct keyboard interface, mouse activation, and indirectly by the application environment, e.g., cut and paste. Updates of the database will be performed as a system administration function. Inputs for updating system tables will be by file transfer protocol (FTP), floppy diskette or 8mm tape.

The principal output will be visual via a display monitor. The classification level will be permanently displayed on each workstation defaulted to the highest classification level processed by the application. All hard copy output will be appropriately labeled at the top and bottom of each page.

Transactions, i.e., production requests, will be replicated by the COTS database software to applicable DoDIIS sites via JWICS/JDISS. Transaction replication will also be made to both peer databases and the central DoDIMS server resident in the DIAC. Should communication downtime occur, output to the central server will be stored and forwarded by each site's replication process upon re-establishment of the communication link.

DoDIMS resides wholly within the DIA in U.S.-only spaces that are authorized for processing of Sensitive Compartmented Information (SCI). All personnel granted unescorted access to the area are cleared to the highest level of data (TS/SCI) to be processes on the DoDIMS AIS. This also matches the highest level of processing of the DIAC LAN and DSNET3/JWICS to which the DoDIMS will be connected.

1.5 (U) AIS Security Summary

Personnel operating and maintaining DoDIMS are cleared for access to TS/SCI material. DoDIMS is located in a DIA SCIF. It satisfies TEMPEST requirements for the facility in which it is located. As a result of certification the system will be connected to the DIA LAN and DSNET3/JWICS which are accredited to operate at the TS/SCI level in the System High Security Mode of Operation. Security functionality of the system is provided by software and provides for user identification and authentication, audit, object re-use, and access control to system, resources. Administrative security procedures are those established for AIS systems operating in the DIAC and for DoDIIS systems. DoDIMS is hosted on a workstation fielded by the JDISS Program Office, Such workstations have been previously certified by DIA for operation at the TS/SCI level in the System High Security Mode of Operation.

2.0 (U) PURPOSE OF TEST

The purpose of the test is to demonstrate that the DoDIMS AIS has implemented sufficient procedural and automated safeguards that will allow it to process TS/SCI data in a System High Mode of Operation with an acceptable level of risk as required by DIAM 50-4 and DCID 1/16. Specifically the objectives of the test are to show that the DoDIMS AIS:

- satisfies the operational and analytic requirements placed on it including for registering, validating, tracking and managing production requirements,

- provides required identification and authentication of all users of the AIS,

- provides sufficient restriction to security sensitive files, and

- provides the capability to retrieve and display audit trail records.

3.0 (U) TEST TEAM

The following persons composed the test team:

Judy C. Crispell, DIA/SY-1D, Test Director
Michael C. Horowitz, DIA/SY-1D, Team Member
John C. Lee, DIA/PO-5C, DoDIMS ISSO and Test Coordinator
Jean M. Layton, DIA/PO-5C, DoDIMS Alternate ISSO and Team Member
Doug Hallford, J.G. Van Dyke & Associates, Inc., DoDIMS Support Staff
Debbie Lambert, J.G. Van Dyke & Associates, Inc., DoDIMS Support Staff
Harry Hiltz, J.G. Van Dyke & Associates, Inc., DoDIMS Support Staff

4.0 (U) TEST RESULTS

4.1 (U) Findings/Requirements

4.2 (U) Discussion

4.3 (U) Recommendations

4.4 (U) Conclusions

5.0 (U) DISPOSITION

A copy of this test report will be forwarded for endorsement through DIA staff channels to DIA/SY-1D prior to granting final certification.

ATTACHMENT A: PROTECTIVE FEATURES

1. (-) Personnel Security

All computer operators and analysts granted access to the DoDIMS AIS are cleared for TOP SECRET and indoctrinated for the SCI compartments processed on the AIS. Military/Government software and hardware maintenance personnel are also cleared System High. Contract maintenance personnel are cleared System High. When this is not possible the DoDIMS AIS and the overall SCIF is or will be sanitized for the duration of the cleared personnel's presence in accordance with established DIAC policy and procedures. Personnel security certification is provided by DIA/DAC.

2. (-) Physical Security

DoDIMS is located in Room B5-911, DIAC, Washington DC. This facility is authorized open storage TS/SCI material and electronic processing of TS/SCI material

3. (-) TEMPEST

(Interim/final TEMPEST accreditation has been provided by DIA/???? per ?????.)

4. (U) Communications Security

The DoDIMS utilizes the DIAC LAN and JWICS for secure data communications.

5. (U) Hardware Security

DoDIMS is hosted on a JDISS Workstation. The JDISS hardware platform is a COTS Sun SPARC workstation. The hardware configuration is described in Attachment B, Description of AIS.

There is no hardware backup to an individual DoDIMS workstation. The operational concept for DoDIMS provides for a master database server and for replication of the DoDIMS database across all active DoDIMS workstations using the Replication Server application software.

Hardware configuration management is accomplished under procedures establishes for DoDIIS systems. There are no inherent hardware security protection features.

6. (U) Software Security

The DoDIMS workstation uses the Solaris OS 4.1.3 and Sybase DBMS 10.0.1 which provide its security functionality.

The major security software features are:

a. USER ID and AUTHENTICATION:

The Solaris OS requires that each user enter an userid and unique password to use system resources. Users are allowed access to applications and data based on their need to know. Access to system files and root privileges is restricted to selected system administrators. The default length of a password is six characters. Passwords are selected by the user from a list of password automatically generated by DIA's SAFE system. Passwords must be changed every six months.

The Sybase DBMS also require a user to enter an userid and password to access the DoDIMS application and data.

b. ACCESS CONTROL

Discretionary access control is enforced by the Solaris OS read, write, execute privileges.

Sybase DBMS access control mechanisms are further used to control user access to DoDIMS data.

c. AUDIT TRAILS

Both Solaris and Sybase maintain audit trails. These audit trails record logon, logoff, access to files/applications as well as action taken such as read, write, execute, change, and delete.

d. LABELING

Data is not labeled within the system. Banner pages with a System High warning are provided. Internal pages of a DoDIMS print job bear classification markings which the system forces the user to specify.

e. DATA/MESSAGE INTEGRITY.

DoDIMS data integrity is provided by the Sybase DBMS. The system is not used to generate AUTODIN messages and therefore has no need to enforce release authority requirements.

f. SANITIZATION/DOWNGRADING

There is no automated sanitization or downgrading of data.

7. (U) Procedural/Administrative Security

a. Message Release Authority. N/A. DoDIMS is not used for transmission or receipt of AUTODIN messages

g. Access Control Procedures. DIA Access Control Procedures govern access to DoDIMS facilities. User Access to the system (authorization to use) is accomplished in accordance with DIAC policies.

c. Data Labels. Any hard copy information printed from the DoDIMS will be handled in accordance with applicable security regulations. Adherence to all existing regulations and guidelines for safeguarding of classified information will continue unchanged.

d. Audit Trail Review and Maintenance. The ISSO periodically reviews all audit trails. Audit trails are maintained on-line for one month and archived off-line on magnetic media in machine readable form for one year.

e. Password/Userid Generation. Userids are issued by the System Administrator in accordance with DoDIIS policy. Passwords are selected by the user from a list that the ISSO generates from the SAFE system. Passwords are changed every six months. Passwords are stored in an encrypted format within DoDIMS.

f. Procedures for removing material from SCIF. Removal of all material from the SCIF is governed by established DIAC procedures.

8. (U) Existing Certifications

JDISS, the host workstation for DoDIMS, has been previously certified by DIA/SY-1D for processing of SCI material in the System High mode of operation.

DoDIMS is not directly connected to another AIS.

ATTACHMENT B: AIS DESCRIPTION

1. (U) Hardware (see also Attachment C)

- Sun SPARCStation 2/10/20 with 32 or 64 MB RAM
- Sun High Resolution Color Monitor
- Sun CD-ROM Drive
- 1.3 GB internal and 2.1 GB external hard drives (minimum)
- Ethernet Transceiver
- Two (2) serial ports
- Bi-directional Printer Port
- 8mm Tape Drive
- Mouse
- NeWSprint CL+ Color Printer

2. (U) Software

COTS:
- SUN OS 4.1.3
- X-windows X11.R5
- OSF Motif 1.2
- Looking Glass Professional 3.0
- ApplixWare 2.1
- ELT/2 2.2.10-R4 with TACO2
- Open Connect TN3270 with graphic option
- TEEMX
- XNVDET
- Sybase 10.0.1
- Sybase Replication Server 10.0.1
- Gain Momentum Runtime
- Newsprint

GFE:
JINTACCS Automated Message Processing Software (JAMPS)

3. (U) Communications Layout

DoDIMS as a Unix-based workstation connected to the DIAC LAN.

4. (U) Functional Arrangement

DoDIMS is a client-server application developed in accordance with DoD and DIA information system architectural standards. It consists of five client modules which reside on a JDISS workstation and a database co-hosted on the workstation.

DoDIMS-unique client software is an application written in Gain Extension Language (GEL) to provide the following modules:

a. Requirements Module. This module provides the user with an automated Production Requirements (PR) process in support of both crisis and non-crisis requests. It provides the intelligence consumer a mechanism to register production requirements and forward them to the appropriate validating organization and, where applicable, any additional authorities. Once validation occurs, a production center is notified of the PR's existence. After reviewing the PR, and coordinating with collaborative production centers if appropriate, the production center sends the consumer a response on the proposed production actions. At any given time, a customer and/or validator has the ability to track the status of the PR through its organization to the producing organization.

b. Assignment Module. As production requirements are fully validated, this module will automatically enter the responsible production center information for assignment based on geographical and functional areas. For requests comprising more than one responsible producer area, the validator will select primary and collaborative producers. This final validating authority is empowered to override the assignment criteria as necessary. DoDIMS will not assign production without an appropriate link to a validated requirement to ensure production resources are being utilized to satisfy consumer requirements.

c. Production Module. This module makes available to the community an on-line production schedule. Production center production managers will have the ability to input and maintain their annual scheduled production. In addition, deconfliction will be accomplished as new information is submitted. An individual entering data will review perceived duplicate entries prior to submitting a new request. As products are published and production schedule records closed-out, cross-reference information will be available to assist the user in retrieving the publication through DoDIIS Dissemination.

d. Reports Module. This module makes available to its users a capability to obtain production management information by utilizing either various pre-defined or user-defined reports. Whatever the type of report, a graphics capability is available consisting of Pie, Bar, Area, line column, and 3-D types of charts.

e. Assessment Module. This module provides a mechanism by which primarily production managers and functional managers obtain information regarding resource utilization, producer assessments, and production shortfalls.

DoDIMS server software consists of Sybase DBMS data tables developed within Sybase, plus the Replication server application.

5. (U) Backup Arrangement

There is no hardware backup to an individual DoDIMS. The operational concept for DoDIMS provides for a master database server and for replication of the DoDIMS database across all active DoDIMS workstations using the Replication Server application software.

6. (U) AIS Use

DoDIMS provides users the ability to: 1) register Production Requests and Intelligence Products initialization/updates, 2) replicate data to DoDIMS sites, and 3) update the peer databases and Central Database.

7. (U) Type and Volume of Classified Material

The type of data stored in the DoDIMS database are categorized as intelligence production questions and responses. Classification labels (including applicable caveats) may be added (selected) by the users of the application. As a default measure, all data entered into the system is classified at the highest level of the system (System High). Classifications can be changed/added to the Request record, Subject and Statement of Requirement of the Request record, the Product record, and the Subject and Abstract of the Product record.

The volume of classified data will vary from site to site and from situation to situation (crisis or non-crisis).

ATTACHMENT C: EQUIPMENT LIST

MANUFACTURER	MODEL	TYPE	QTY	SERIAL NO.

Site Dependent

ATTACHMENT D: COMMUNICATIONS DIAGRAMS

Not Applicable

ATTACHMENT E: FUNCTIONAL DIAGRAMS

Not Applicable

ATTACHMENT F: BACKUP CONFIGURATION DIAGRAMS

Not Applicable